(TS//SI) MASTERSHAKE: Locating Terrorists at Internet Cafés

FROM: [redacted]
SIGDEV/Network Analysis Center (S31SD)
Run Date: 05/26/2005

Zeroing in on terrorists who use public internet terminals. (TS//SI)

(S//SI) During a recent TDY to Iraq, a group of SID leaders met with the Charge D'Affairs at the embassy in Baghdad. As related by MG Quirk, the official "spent a lot of time with us, and was very forthcoming with his needs." The first three priorities on his list were "Where is Zarqawi?", "Where is Zarqawi?" and "Where is Zarqawi?" (See the article MGQ's Notes from the Field .)

(TS//SI) So what is SID doing to help locate terrorists in Iraq? One effort underway is a project called MASTERSHAKE. MASTERSHAKE maintains detailed technical information, as well as business-related information, for devices which provide connectivity to the public Internet. The vast majority of Iraqi Internet cafés are connected to the public Internet via satellite dishes and modems which use Digital Video Broadcast - Satellite (DVBS) technologies. As a product of the way these connections are made, providers who operate these hubs and their services require "rough" geolocation information for the installation of the modem. MASTERSHAKE targets the entire business chain, from manufacturer to Internet café installation, to ascertain any and all available data regarding this geolocation, the network connectivity of the modem, as well as the actual physical location of the installation.

(TS//SI) That's not the only source for that information, though! MASTERSHAKE also fuses a variety of data sources from across SID organizations and intelligence agencies to enrich its knowledge of each particular installation. Additionally, Network Analysis Center (NAC) analysts are using RAD's X-Keyscore system to develop more precise location information by studying the entirety of the network environment being served by each of these modems.

(TS//SI) MASTERSHAKE enriches and maintains all of this technical and geolocation information and uses a unique hardware identifier of the satellite modem, called the Media Access Control (MAC) address, to provide target offices with its best knowledge of the actual physical destination of each and every session in which they see identifiers relating to their target. In some cases, MASTERSHAKE can locate the target to a particular seat within an Internet café. Currently, MASTERSHAKE contains:

- Technical detail on over 9,000 satellite modems in the Middle East and Africa, many locatable to a particular city
- Precise location information on over 400 Internet cafés
- Seat-level identification for over 50 cafes

(TS//SI) The locational information is accessible locally, as well as provided to TRAFFICTHIEF, a system that provides near real-time alerts to analysts and war fighters on the ground telling them when and where high-value targets are active on the global net if detected via any SIGINT access such as SCS , TAO , RFO , SSO , etc. (See related article .) This information is used by local and regional analysts to inform forward deployed elements so that they can conduct surveillance and rendition operations.

(TS//SI) To date, MASTERSHAKE has been a part of over 80 SIGINT-enabled operations which have resulted in numerous arrests, and information from MASTERSHAKE contributes daily to operations in Iraq. Here's one example: In late December 2004, counterterrorism target "Hamzah" sent messages from a computer geolocated to a café in Ramadi, and the café was put under SIGINT-enabled surveillance. On 15 January 2005, two counterterrorism targets went to the internet café and began using "messenger" services. A TRAFFICTHIEF tipper -- incorporating MASTERSHAKE locational information -- was issued, and [redacted] the two men

were arrested.

(U//FOUO) If you have questions about MASTERSHAKE, please contact [redacted] of the Network Analysis Center at [redacted]
